

1 CLAIMS

2 1. A method comprising:

3 achieving agreement among n participating network devices in an asynchronous network
4 for deciding on a common value (v) being validated by a justification (p) together
5 satisfying a predetermined predicate (Q), a agreement arising out of a series of
6 messages being sent and received by each participating network device with up to a
7 number t of faulty devices, each participating network device performing the
8 following steps:

9 i) broadcasting to the participating network devices an echo message comprising a
10 proposed value (w) and a proposed justification (π) by using verifiable and
11 consistent broadcast;

12 ii) receiving $n-t$ echo messages comprising candidate values (w_1, w_2, w_3) and
13 candidate justifications (π_1, π_2, π_3) satisfying the predicate (Q), and
14 repeating the following steps 1) to 3) for each participating network device as a
15 candidate device represented by a candidate device identifier (a) according to an
16 order:

17 1) broadcasting to all participating network devices a vote message comprising
18 the candidate device identifier (a), and either a first agree-value (Y) together
19 with the candidate value (w_a) and the candidate justification (π_a), or a second
20 agree-value (N),

21 2) receiving vote messages and counting up to $n-t$ vote messages including the
22 second agree-value (N) or the first agree-value (Y), the candidate value (w_a),
23 and the candidate justifications (π_a) satisfying the predicate (Q),

24 3) performing a Byzantine agreement to determine whether the candidate device
25 has sent the candidate value (w_a) and the candidate justification (π_a) satisfying
26 the predicate (Q),

1 iii) in response to the result of the Byzantine agreement, deciding the common value
2 (v) proposed as the candidate value (w) and the justification (p) proposed as the
3 candidate justification (π) of an agreed candidate device.

4 2. Method according to claim 1, whereby step ii) further comprises
5 - broadcasting a commit message comprising sender identities of received echo
6 messages,
7 - receiving commit messages,
8 - selecting randomly the order of the candidate device by opening at least one
9 cryptographic common coin,
10 - and whereby in step 2) the vote messages are counted which are consistent with
11 the received commit messages.

12 3 Method according to claim 2, whereby the step of opening at least one cryptographic
13 common coin comprises using a distributed coin-tossing protocol.

14 4. Method according to claim 1, whereby in step i) the verifiable and consistent
15 broadcast comprises a certified delivery of the broadcasted echo message within a
16 sent message and reaching agreement on the content of the broadcasted echo
17 message.

18 5. Method according to claim 1, whereby in step i) the verifiable and consistent
19 broadcast comprises exchanging signed messages between the participating network
20 devices .

21 6. Method according to claim 1, whereby in step i) the verifiable and consistent
22 broadcast comprises using threshold signatures.

- 1 7. Method according to claim 1, whereby steps 1) and 2) in step ii) comprise
2 broadcasting the candidate value (w_a) and the candidate justification (π_a) upon a
3 request.
- 4 8. Method according to claim 1, whereby in step ii) the participating network devices
5 are voting on several candidate devices simultaneously.
- 6 9. A method for reliably broadcasting messages in an order within an asynchronous
7 network comprising n participating network devices and tolerating a number t of less
8 than $n/3$ faulty participating network devices, each participating network device
9 storing a queue (q) and a log (d), the method operating in rounds, each round
10 comprising the following steps:
11 i) responsive to a message broadcast request comprising a message value (m)
12 performing the step of:
13 appending the message value (m) to the queue (q) unless the log (d) or the
14 queue (q) comprises the message value (m),
15 ii) deriving a signature (σ) on the queue (q),
16 iii) broadcasting to all participating network devices a queue message comprising
17 the queue (q) and the signature (σ),
18 iv) receiving a number c of at least $t+1$ queue messages comprising c proposed
19 queues and proposed signatures ,
20 v) storing the proposed queues in a queue vector (QV) and the proposed signatures
21 in a signature vector (SV),
22 vi) proposing the queue vector (QV) for Byzantine agreement validated by the
23 signature vector (SV) and performing a method for achieving agreement on a
24 common value being validated by a justification (p) together satisfying a
25 predetermined predicate (Q) by validating the queue vector (QV) and the
26 signature vector (SV) through a determined predicate (Q) asserting that the

- 1 signature vector (SV) comprises c valid signature entries of distinct
2 participating network devices (A, B, C) on entries of the queue vector (QV),
3 vii) preparing in response to the result of the Byzantine agreement an ordered list
4 (L) of unique message values out of the entries of the decided queue vector
5 (DQV)
6 viii) accepting the unique message values in the ordered list (L) in the sequence of
7 the ordered list (L),
8 ix) appending the accepted unique message values to the log (d).

9 10. Method according to claim 9, whereby step of performing a method for achieving
10 agreement on a common value comprises:

11 achieving agreement among n participating network devices in an asynchronous network
12 for deciding on a common value (v) being validated by a justification (p) together
13 satisfying a predetermined predicate (Q), the agreement arising out of a series of
14 messages being sent and received by each participating network device with up to a
15 number t of faulty devices, each participating network device performing the
16 following steps:

- 17 i) broadcasting to the participating network devices an echo message comprising a
18 proposed value (w) and a proposed justification (π) by using verifiable and
19 consistent broadcast;
20 ii) receiving $n-t$ echo messages comprising candidate values (w_1, w_2, w_3) and
21 candidate justifications (π_1, π_2, π_3) satisfying the predicate (Q), and
22 repeating the following steps 1) to 3) for each participating network device as a
23 candidate device represented by a candidate device identifier (a) according to an
24 order:

- 1 2) broadcasting to all participating network devices a vote message comprising
- 2 the candidate device identifier (a), and either a first agree-value (Y) together
- 3 with the candidate value (w_a) and the candidate justification (π_a), or a second
- 4 agree-value (N),
- 5 2) receiving vote messages and counting up to $n-t$ vote messages including the
- 6 second agree-value (N) or the first agree-value (Y), the candidate value (w_a),
- 7 and the candidate justifications (π_a) satisfying the predicate (Q),
- 8 3) performing a Byzantine agreement to determine whether the candidate device
- 9 has sent the candidate value (w_a) and the candidate justification (π_a) satisfying
- 10 the predicate (Q),
- 11 iii) in response to the result of the Byzantine agreement, deciding a common value
- 12 (v) proposed as the candidate value (w) and the justification (p) proposed as the
- 13 candidate justification (π) of an agreed candidate device.

14 11. Method according to claim 9, whereby step iv) further comprises appending an
15 unknown message value found in a received queue message to the queue (q) unless
16 the log (d) or the queue (q) comprises the unknown message value.

17 12. Method according to claim 1, whereby the number t of faulty devices is extended to a
18 set T of sets comprising participating network devices.

19 13. Method according to claim 12, whereby the participating network devices show
20 hybrid failures (BF, CF, LF) reflecting a different structure of the set T or different
21 thresholds t_i , with $i = 1, 2, \dots, L$.

22 14. An article of manufacture comprising a computer usable medium having computer
23 readable program code means embodied therein for causing achievement of

1 agreement, the computer readable program code means in said article of manufacture
2 comprising computer readable program code means for causing a computer to effect
3 the steps of claim 1.

4 15. An article of manufacture comprising a computer usable medium having computer
5 readable program code means embodied therein for causing reliable broadcasting of
6 messages, the computer readable program code means in said article of manufacture
7 comprising computer readable program code means for causing a computer to effect
8 the steps of claim 9.

9 16. Method according to claim 9, whereby the number t of faulty devices is extended to a
10 set T of sets comprising participating network devices.

11 17. Method according to claim 16, whereby the participating network devices show
12 hybrid failures (BF, CF, LF) reflecting a different structure of the set T or different
13 thresholds t_i , with $i = 1, 2, \dots, l$.

14 18. A program storage device readable by machine, tangibly embodying a program of
15 instructions executable by the machine to perform method steps for causing
16 achievement of agreement, said method steps comprising the steps of claim 1.

17 19. A program storage device readable by machine, tangibly embodying a program of
18 instructions executable by the machine to perform method steps for causing reliable
19 broadcasting of messages, said method steps comprising the steps of claim 9.

20 20. A system comprising:

1 means for achieving agreement among n participating network devices in an
2 asynchronous network for deciding on a common value (v) being validated by a
3 justification (p) together satisfying a predetermined predicate (Q), the agreement
4 arising out of a series of messages being sent and received by each participating
5 network device with up to a number t of faulty devices, each participating network
6 device including:

7 i) means for broadcasting to the participating network devices an echo message
8 comprising a proposed value (w) and a proposed justification (π) by using
9 verifiable and consistent broadcast;

10 ii) means for receiving $n-t$ echo messages comprising candidate values (w_1, w_2, w_3)
11 and candidate justifications (π_1, π_2, π_3) satisfying the predicate (Q), and
12 repeating the following steps 1) to 3) for each participating network device as a
13 candidate device represented by a candidate device identifier (a) according to an
14 order:

15 3) means for broadcasting to all participating network devices a vote message
16 comprising the candidate device identifier (a), and either a first agree-value
17 (Y) together with the candidate value (w_a) and the candidate justification (π_a),
18 or a second agree-value (N),

19 2) means for receiving vote messages and counting up to $n-t$ vote messages
20 including the second agree-value (N) or the first agree-value (Y), the
21 candidate value (w_a), and the candidate justifications (π_a) satisfying the
22 predicate (Q),

23 3) means for performing a Byzantine agreement to determine whether the
24 candidate device has sent the candidate value (w_a) and the candidate
25 justification (π_a) satisfying the predicate (Q),

26 iii) means for deciding in response to the result of the Byzantine agreement, the
27 common value (v) proposed as the candidate value (w) and the justification (p)
28 proposed as the candidate justification (π) of an agreed candidate device.

1 21. A computer program product comprising a computer usable medium having
2 computer readable program code means embodied therein for causing achievement of
3 agreement, the computer readable program code means in said computer program product
4 comprising computer readable program code means for causing a computer to effect the
5 functions of claim 20.

CH920000062US1